This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2017.2777470, IEEE Transactions on Multimedia

# HEVC Selective Encryption Using RC6 Block Cipher Technique

**Ahmed I. Sallam**
Department of Computer Science & Engineering
Faculty of Electronic Engineering, Menoufia University
Menouf, Egypt
a_sallam82@hotmail.com
**Osama S. Faragallah**
Department of Computer Science & Engineering
Faculty of Electronic Engineering, Menoufia University
Menouf, Egypt
Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 888, Al-Hawiya 21974, Kingdom of Saudi Arabia
osam_sal@yahoo.com, o.salah@tu.edu.sa

**El-Sayed M. EL-Rabaie**
Department of Electronic and Communication Engineering
Faculty of Electronic Engineering, Menoufia University
Menouf, Egypt
Srabie1@yahoo.com

***Abstract*— The High-Efficiency Video Coding (HEVC) selective encryption (SE) technique depends on encrypting the highly sensitive data on the video bit stream. The HEVC SE technique should keep the video format compliance, same bit rate, and real-time constraints. This paper presents an efficient RC6-based HEVC SE technique that encrypts the sensitive video bits with the features of low complexity overhead, fast encoding time for real-time applications and keeping the HEVC constant bitrate with format compliant. These features result from using the low computational complexity RC6 block cipher for encrypting the selective video bins. The proposed RC6-based HEVC SE encrypts the Discrete Cosine Transform (DCT) coefficients sign bits, the DCT remaining absolute values suffixes that are binarized by Exp-Golomb (EGk) order zero (EG0), the Motion Vector Difference (MVD) sign bits and MVD absolute values suffixes that are binarized by EGk order one (EG1). Also, this paper introduces experimental results that compare between the proposed RC6-based HEVC SE and the HEVC SE algorithms that use the Advanced Encryption Standard (AES) in different operation modes. This paper presents more details about the security analysis of the proposed RC6-based HEVC SE including the encryption quality analysis, the key space analysis, statistical analysis like histogram and correlation coefficient analysis and sensitivity analysis like the key sensitivity analysis. The achieved test results ensured and confirmed the security, reliability, and robustness of the proposed RC6-based HEVC SE technique.**

***Keywords—Video compression, HEVC, context adaptive binary arithmetic coding (CABAC), Video encryption, Selective encryption, RC6, Advanced Encryption Standard (AES).***

## I. Introduction

The HEVC is the most recent video coding standard which was published in 2013 by Joint Collaborative Team on Video Coding (JCT-VC) between the ITU-T VCEG and the ISO/IEC MPEG [1]. The main feature of the HEVC is to increase the video compression ratio with keeping the same video quality compared to the H.264/AVC standard [2]. Nowadays, the security of the video content has been a challenging research topic. The simple way for securing the video content is to encrypt all video bitstream using an encryption algorithm without considering the video coding structure that is defined as Naive Encryption Algorithm (NEA) [3]. The NEA algorithm has drawbacks of large computationally cost of encryption/decryption processes and removing the video format compliance. So, there is an urgent need for the selective video encryption that is used as an alternative for the NEA. The selective video encryption depends on the structure of the video coding for encrypting only the highly sensitive video bitstream [4].

The SE should guarantee the visual distortion of the video content with keeping the format compliance of the video encoding/decoding processes. Also, the SE should ensure that the bit rate of the ciphervideo is the same as the bit rate of the plainvideo. The format compliance means that the ciphervideo should keep the HEVC video coding structure and any standard HEVC decoder can decode the ciphervideo bitstream without the need for the decryption process. The format compliance is important for supporting various video operations like watermarking, cutting and copying on the ciphered HEVC video. Not all the syntax elements in the HEVC can be encrypted with ensuring the format compliance condition. So we should choose the syntax elements that preserve the format compliance to be encrypted. These syntax elements like Short-term reference picture set (RPS), Quantization Parameter (QP), Delta Quantization Parameter (delta QP) for the slice and the CU, motion vector sign, motion vector difference, DCT coefficients signs, Deblocking and SAO filters parameters [5]. In the HEVC video encoding process, the last stage of the process is the entropy coding. The entropy coding performs a lossless compression by using the statistical properties for compressing the video data. This means that few bits can represent the frequently used data while many bits can represent the infrequently used data. The HEVC video coding uses the context-based adaptive binary arithmetic coding (CABAC) for the entropy process [6].

Most of the HEVC SE techniques investigate the HEVC video coding structure and encrypt the most sensitive syntax elements in the video bitstream.

Heinz Hofbauer [7], proposed a HEVC SE technique that is based on encrypting the AC DCT coefficients sign bits in the luminance channel. This technique flips the sign bits of only the AC DCT coefficients randomly based on a specified percentage of signs in the bit stream.

Yiqi Tew [8], modified the technique in [7] and proposed a HEVC SE technique that is based on encrypting the transform skip signal and sign bit in format compliance manner. This technique uses a shared secret key as an input to hash function and output the hash value that is used to flip the transform skip signal and the sign bits of the AC DCT coefficients in the luminance channel and the MVD.

Z. Shahid.W. Puech [9], introduced a HEVC SE technique that depends on encrypting the selective binstrings in the CABAC with a format compliance mode. This technique encrypts the truncated rice binstrings of the quantized transform coefficients (QTCs) by AES in CFB (Cipher Feedback) mode [10].

Glenn [11], proposed a HEVC SE technique that based on encrypting specific syntax elements that do not modify the entropy decoding process to keep the video format compliance. These syntax elements like the RPS on the slice header, QP information on the CU Level, Inter information (reference picture indices, MVD) on the PU level, Residual information on the TU level, deblocking filter parameters and Sample adaptive offset parameters on the slice level.

Most of HEVC SE techniques encrypt the syntax elements in the entropy process using the encryption standard algorithms like AES or DES (Data Encryption Standard).

The binarization process converts the non-binary syntax element to binary strings that is defined as bin-strings. In HEVC, there are five binarization methods defined as the fixed length code, Unary code, Truncated Unary (TU) Binarization, EGk Binarization and Truncated Rice (TR) Binarization. Each syntax element is assigned to use a specific binarization method to be mapped to its binary values. Table 1 will give an example for using the five binarization methods for mapping an unsigned integer N to its binary values [12-13].

TABLE 1: EXAMPLES OF BINARIZATIONS METHODS [12].

| *N* | Fixed-Length (FL) cMax = 7 | Unary (U) | Truncated Unary (TrU) cMax = 7 | Exp-Golomb (EGk) K=0 | Truncated Rice (TRk) k = 1; cMax = 7 |
|---|---|---|---|---|---|
| **0** | 000 | 0 | 0 | 1 | 00 |
| **1** | 001 | 10 | 10 | 010 | 01 |
| **2** | 010 | 110 | 110 | 011 | 100 |
| **3** | 011 | 1110 | 1110 | 00100 | 101 |
| **4** | 100 | 11110 | 11110 | 00101 | 1100 |
| **5** | 101 | 111110 | 111110 | 00110 | 1101 |
| **6** | 110 | 1111110 | 1111110 | 00111 | 1110 |
| **7** | 111 | 11111110 | 1111111 | 0001000 | 1111 |

The RC6 is a symmetric key block cipher that was developed in 1998 to be in competition the AES [14]. It depends on two Feistel networks whose data are mixed via data dependent rotations. The RC6 has flexible round number and block, a key size that can be changed easily. The RC6 has four registers with a 32-bit length that help in performing two rotations/round. The RC6 is defined as RC6-w/r/b where w is denoted as word size in bits, r is denoted as the number of round and b is denoted as the length of the key in bytes. The encryption key with length b is divided into sub keys and loaded into array S[0, ..., 2r + 3]. The plaintext is stored into four registers called (A, B, C, D) [15-16]. When the plaintext is larger than the fixed block size, the plaintext is divided into blocks that can be encrypted one at a time. Modes of operation define how the output of one round is used as input to the next round. The modes of operation are Electronic Code Book (ECB), Cipher Block Chaining (CBC), CFB, Output Feedback (OFB), and Counter (CTR) [17-19].

This paper presents an efficient proposed HEVC SE using the feature of low complexity overhead of the RC6 block cipher to encrypt the DCT coefficients sign bits, the DCT remaining absolute value suffixes that is binarized by EG0, the MVD sign bits and MVD absolute value suffixes that is binarized by EG1. The contribution of the proposed RC6-based HEVC SE is to encrypt the sensitive video bits with the features of low complexity overhead for using in real-time video applications, fast encoding time, keeping the HEVC constant bitrate and format compliant.

The rest of this paper is organized as follows: Section 2 provides the proposed RC6-based HEVC SE technique. Section 3 introduces the performance studies that were instrumented to compare the RC6-based HEVC SE and the previous HEVC SE techniques that use the AES in different operation modes. Section 4 presents the security analysis of the proposed RC6-based HEVC SE technique. Section 5, concludes the paper, followed by the more relevant references.

## II. THE PROPOSED RC6-BASED HEVC SE TECHNIQUE

The proposed RC6-based HEVC SE uses the RC6 block cipher for encrypting a group of the bins that use the bypass-BAC mode in the entropy process to ensure the format compliance, same bit rate, and real-time constraints. From the binarization techniques, the truncated rice code with context (TRp) and EGk code can fulfill these constraints of the HEVC SE. The unary and truncated unary techniques do not meet the same bit rate constraint because they have different code lengths for each input value. The fixed length technique does not meet the format compliance constraint because it is used for binarization of the header syntax and any changes in the header will affect the format compliance. The RC6-based HEVC SE encrypts the DCT coefficients sign bits, the DCT remaining absolute value suffixes that are binarized by EG0, the MVD sign bits and MVD absolute value suffixes that are binarized by EG1. It encrypts these syntax elements because any modification of the suffix (division remainder) and the sign bin (one bit) does not change the format compliance and keeps the same bit rate. It uses the RC6 block cipher because it has a low time delay and low computational complexity that meet the real-time constraint. It performs the encryption process in each entropy slice independently before the compression by BAC because the context model is reset every entropy slice. Fig. 1 shows the block diagram of the proposed RC6-based HEVC SE technique.

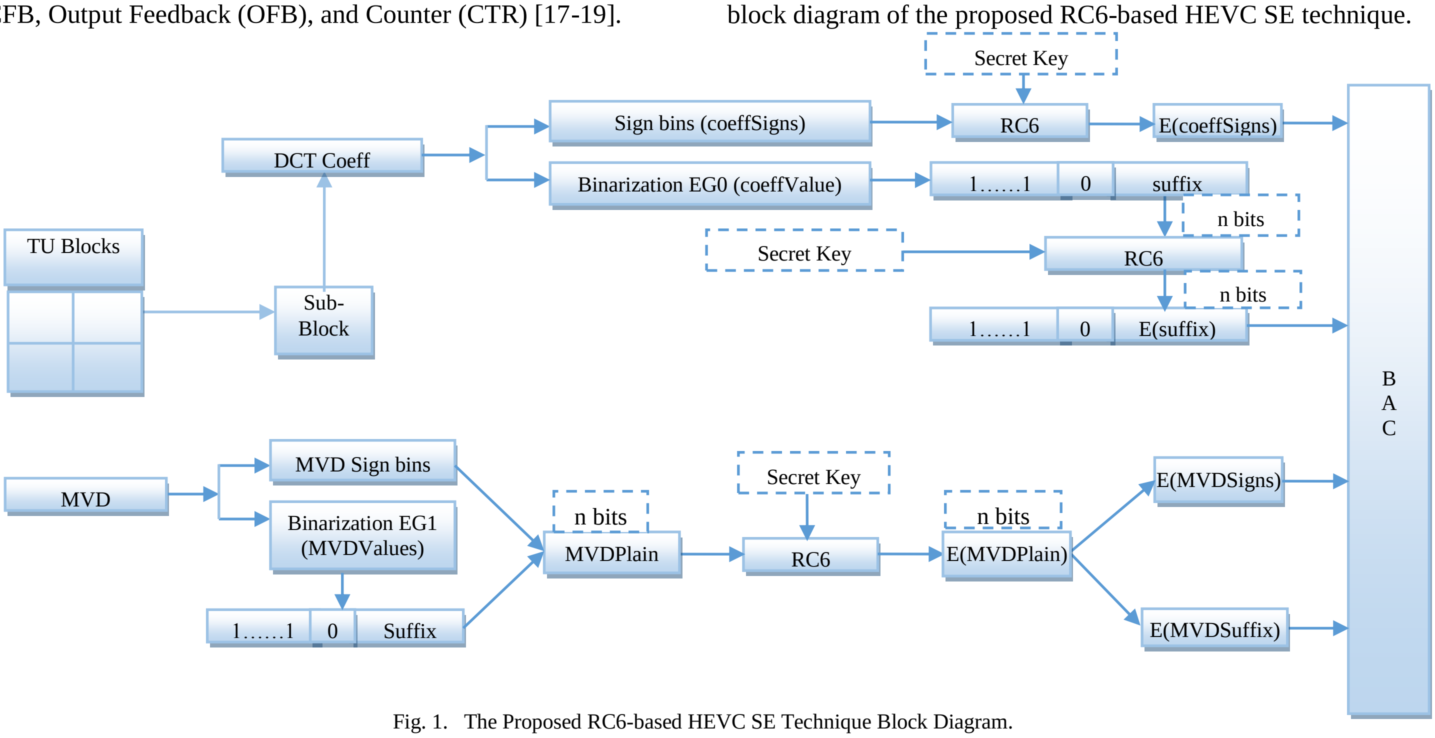



Fig. 1. The Proposed RC6-based HEVC SE Technique Block Diagram.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2017.2777470, IEEE Transactions on Multimedia

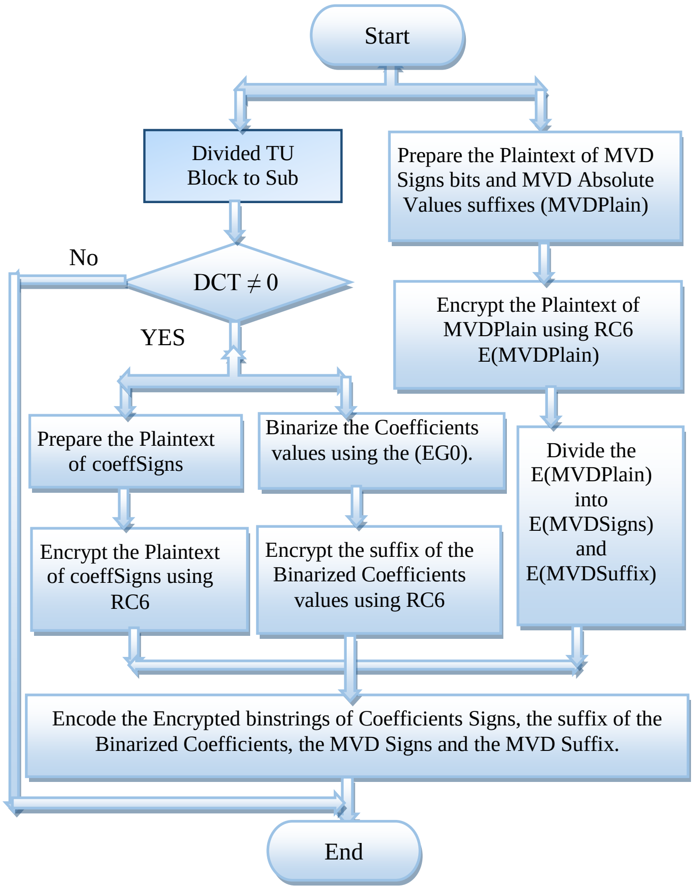



Fig. 2. The Flowchart for the Proposed RC6-Based HEVC SE Technique.

Fig. 2 presented the flowchart of the proposed RC6-based HEVC SE technique. The RC6-based HEVC SE is described as follows:

- Encryption of the Non-Zero DCT coefficients sign bits and the DCT remaining absolute value suffixes that are binarized by EG0.

1- Divided the transform unit (TU) of NxN blocks to 4x4 sub-blocks that contain the DCT coefficients.
2- For each sub-block, prepare the plaintext of the DCT coefficients signs (coeffSigns) bitstring by the following:
   coeffSigns = 2 * coeffSigns + ( CoeffValue < 0 ? 1:0 ).
3- Encrypt the coeffSigns by using the RC6 block cipher algorithm to generate E(coeffSigns) with the same length.
4- Encode the E(coeffSigns) instead of the original coeffSigns.
5- For each Non-Zero coefficient in DCT coefficients of the sub-block:
   If the DCT coefficient absolute value > baseLevel where baseLevel = {7; 14; 26; 46; 78}.
   • Set coeffValue = DCT coeff – baseLevel.
   • Binarization for the coeffValue by using the EG0.
6- Encrypt the suffix of the EG0 of the coeffValue by using the RC6 block cipher algorithm to generate E(suffix) with the same length.
7- Encode the E(suffix) instead of the original the suffix of the coeffValue.

- Encryption of the MVD sign bits and the MVD absolute value suffixes that are binarized by EG1.

1- Prepare the plain string by concatenating the horizontal and vertical MVD sign bits and the horizontal and vertical MVD absolute value suffixes (MVDPlain).
2- Encrypt the plain string by using the RC6 block cipher to generate cipher string with the same length E(MVDPlain).
3- Divide the cipher string into the cipher horizontal and vertical MVD sign bits E(MVDSigns) and the cipher horizontal and vertical MVD absolute value suffixes E(MVDSuffix).
4- Encode the cipher horizontal and vertical MVD sign bits and the cipher horizontal and vertical MVD absolute value suffixes instead of the original bins.

As shown in Fig. 1, the encryption space for the proposed RC6-based HEVC SE technique consists of the non-zero DCT coefficients sign bits, the non-zero DCT remaining absolute value suffixes that are binarized by EG0, the MVD sign bits and MVD absolute value suffixes that are binarized by EG1.

The contribution of the RC6-based HEVC SE technique is to encrypt the HEVC video content with keeping the format compliance, same bit rate, and real-time constraints. This contribution is achieved by the following:

- The format compliance constraint is achieved by encrypting the binstrings in the encryption space that use the bypass-BAC mode in the entropy process and don't modify the HEVC video coding structure as descried at the first of this section.
- The same bit rate constraint is achieved by encrypting the DCT coefficients sign bits, the DCT remaining absolute value suffixes that are binarized by EG0, the MVD sign bits and MVD absolute value suffixes that are binarized by EG1 that ensure the encrypted bins have the same length of the original bins.
- The real-time constraint is achieved by using the RC6 block cipher which is fast and simple structure encryption algorithm.
- The proposed method uses the RC6 block cipher to save the time of the conversion of non-dyadic encryption space to dyadic encryption space process in the Z. Shahid [9] algorithm due to using the AES-CFB encryption algorithm.

## III. PERFORMANCE STUDY

There are many objective video quality measurements like the SSIM and PSNR metrics that can be used to study the performance of various video coding techniques [20]. This section describes our performance experiments to measure the scrambling performance and the encoding time between the RC6-based HEVC SE technique and other techniques in the previous related work that uses the AES in different modes of operations like CFB, CBC, ECB, OFB and CRT. The RC6-based HEVC SE technique and the techniques in previous related work are implemented by applying the encryption on the HM16.0 reference software [21]. The machine that is used in our implementation has the following specifications (CPU speed 3.4 GHz core i7, physical RAM size 6 GB and hard disk size 500 GB). Table 2 defines the video sequences that are used in the performance study. The encoding parameters are described in Table 3. These experiments use the MSU Video Measurement Tool to measure the PSNR and the SSIM metrics [24].

TABLE 2: PERFORMANCE STUDY VIDEO SEQUENCES [22-23].

| Frame Sequence | Resolution | Frame Per Second |
|---|---|---|
| Bosphorus | 3840 X 2160 | 120 fps |
| Jockey | 1920 X 1080 | 120 fps |
| FourPeople | 1280 X 720 | 60 fps |
| Mobcal | 720 X 576 | 25 fps |
| Forest | 320 X 240 | 30 fps |

TABLE 3: ENCODING PARAMETERS VALUES.

| Parameter | Value |
|---|---|
| Profile | Main |
| Configuration | Low Delay for real time applications |
| Group of Picture (GOP) | Four frames consists of One I Frame followed by three B frames |

### A. ENCODING TIME EXPERIMENTAL RESULTS

Table 4 illustrates the measurement of the average encoding time per one frame in seconds of the RC6-based HEVC SE technique and the other previous related work that uses the AES in different operation modes.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2017.2777470, IEEE Transactions on Multimedia

TABLE 4: AVERAGE ENCODING TIME PER FRAME IN SECONDS OF THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES.

| Technique / Video Sequence | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| **Bosphorus** | 2320 | 2339 | 2531 | 2530 | 2343 | 2441 |
| **Jockey** | 505 | 510 | 538 | 540 | 513 | 511 |
| **FourPeople** | 248 | 253 | 282 | 281 | 255 | 254 |
| **Mobcal** | 206 | 216 | 273 | 272 | 215 | 217 |
| **Forest** | 25.8 | 26.5 | 30.2 | 30.1 | 26.8 | 26.6 |

The RC6-based HEVC SE technique has an encoding time lower than the previous technique that uses the AES in different modes of operation like CFB, CBC, ECB, OFB and CRT. Table 4 illustrated that the RC6-based HEVC SE technique saved the average encoding time for one frame by 0.7 sec and 4.4 sec compared with AES-CFB and AES-CBC, respectively for the low-resolution Forest video (320 X 240). Also, the RC6-based HEVC SE technique saves the average encoding time for one frame by 19 sec and 211 sec compared with AES-CFB and AES-CBC for the high-resolution Bosphorus video (3840 X 2160).

These results are due to using the RC6 block cipher which is fast and simple structure encryption algorithm and saving the time of the conversion of non-dyadic encryption space to dyadic encryption space process when using the AES-CFB [9].

Also, Table 4 presented the average encoding time for only one frame of the video sequence at different resolution. So, if we have one video with 100 frames, the time saving will be 70 sec and 440 sec compared with AES-CFB and AES-CBC for the low-resolution Forest video (320 X 240). Also, the time saving will be 1900 sec and 21100 sec compared with AES-CFB and AES-CBC, respectively for the high-resolution Bosphorus video (3840 X 2160). This indicates that the more numbers of the video frames, the more time saving by using the proposed RC6-based HEVC SE technique.

The long time in Table 4 is due to using the HM16.0 reference software without software packaging. The HM16.0 reference software is developed by JCT-VC team to be used as reference implementation of the HEVC standard encoding and decoding process. The HM16.0 reference software is developed for implementing the HEVC in the research field not to be used in the commercial field [21].

## B. PSNR And SSIM EXPERIMENTAL RESULTS

Tables 5 and 6 illustrate the measurements of the average PSNR and SSIM of the RC6-based HEVC SE technique and the related previous HEVC SE technique that uses the AES in different operation modes for video sequences in Table 2.

TABLE 5: AVERAGE PSNR OF THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES FOR THE VIDEO SEQUENCES IN TABLE 2.

| Technique / Video Sequence | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| **Bosphorus** | 10.83 | 7.8 | 11.16 | 6.27 | 7.8 | 7.8 |
| **Jockey** | 8.63 | 9.41 | 9.88 | 9.41 | 9.41 | 9.41 |
| **FourPeople** | 10.6 | 9.76 | 8.82 | 5.96 | 9.76 | 9.76 |
| **Mobcal** | 11.79 | 7.49 | 11.32 | 11.3 | 7.49 | 7.49 |
| **Forest** | 12.11 | 10.4 | 12.81 | 11.46 | 10.4 | 10.4 |

TABLE 6: AVERAGE SSIM OF THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES FOR THE VIDEO SEQUENCES IN TABLE 2 .

| Technique / Video Sequence | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| **Bosphorus** | 0.186 | 0.166 | 0.244 | -0.048 | 0.166 | 0.166 |
| **Jockey** | 0.020 | 0.086 | 0.060 | -0.007 | 0.086 | 0.086 |
| **FourPeople** | 0.064 | 0.069 | 0.050 | -0.051 | 0.069 | 0.069 |
| **Mobcal** | 0.028 | 0.092 | 0.361 | 0.185 | 0.092 | 0.092 |
| **Forest** | 0.073 | 0.183 | 0.147 | 0.043 | 0.183 | 0.183 |

Tables 7 and 8 illustrate the measurements of the average PSNR and SSIM of the proposed RC6-based HEVC SE technique and the other previous related work that uses the AES in different operation modes for the FourPeople video sequence with resolution of 1280 x 720 at different QP values.

TABLE 7: AVERAGE PSNR OF THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES FOR THE FOURPEOPLE VIDEO AT DIFFERENT QP VALUES.

| Technique / QP | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| **22** | 6.43 | 8.68 | 11.16 | 8.67 | 8.68 | 8.68 |
| **27** | 8.69 | 10.79 | 7.11 | 9.84 | 10.79 | 10.79 |
| **32** | 5.91 | 8.67 | 8.2 | 8.27 | 8.67 | 8.67 |
| **37** | 8.15 | 9.35 | 10.12 | 7.98 | 9.35 | 9.35 |

TABLE 8: AVERAGE SSIM OF THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES FOR THE FOURPEOPLE VIDEO AT DIFFERENT QP VALUES.

| Technique / QP | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| **22** | 0.106 | 0.016 | 0.047 | -0.017 | 0.016 | 0.016 |
| **27** | 0.044 | 0.050 | -0.040 | 0.051 | 0.050 | 0.050 |
| **32** | 0.045 | 0.002 | 0.062 | -0.014 | 0.002 | 0.002 |
| **37** | 0.028 | 0.070 | -0.04 | 0.050 | 0.070 | 0.070 |

Tables 5, 6, 7 and 8 showed that the RC6-based HEVC SE technique has a visual distortion for the original video with a slight difference of that is generated by using the AES in different modes of operation. The ciphervideo generated by the RC6-based HEVC SE technique has lower average PSNR and higher average SSIM than the ciphervideo that is generated by using the AES in different modes of operation. The experimental results shows that the RC6-based HEVC SE scheme saves the average frame encoding time with remaining of the near visual distortion of the ciphervideo stream by the previous technique that uses the AES as seen with slight difference PSNR and SSIM values. Fig. 3 shows the FourPeople plainvideo/ciphervideo using the RC6-based HEVC SE technique at different QP.

a) The FourPeople plainvideo Frame # 50

b) The FourPeople ciphervideo Frame # 50 using the proposed RC6-based HEVC SE Technique with QP=22

c) The FourPeople ciphervideo Frame # 50 using the proposed RC6-based HEVC SE Technique with QP=27

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2017.2777470, IEEE Transactions on Multimedia

d) The FourPeople ciphervideo Frame # 50 using the proposed RC6-based HEVC SE Technique with QP=32

e) The FourPeople ciphervideo Frame # 50 using the proposed RC6-based HEVC SE Technique with QP=37

Fig. 3. The FourPeople Ciphervideo Using the RC6-based HEVC SE Technique at Different QP Values.

## IV. SECURITY ANALYSIS

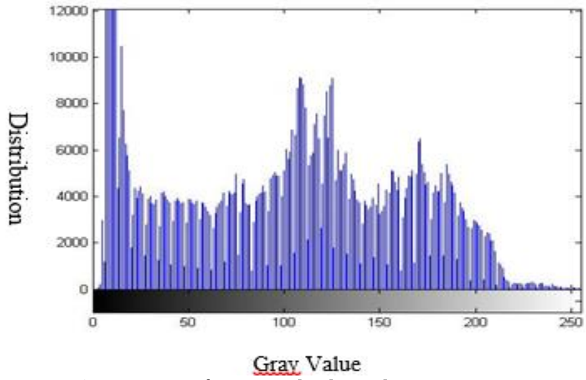
This section introduces the security analysis of the RC6-based HEVC SE technique like key space analysis, statistical analysis, and sensitivity analysis to ensure the security and the robustness of the proposed technique against the most common attacks.

### A. KEYSPACE ANALYSIS

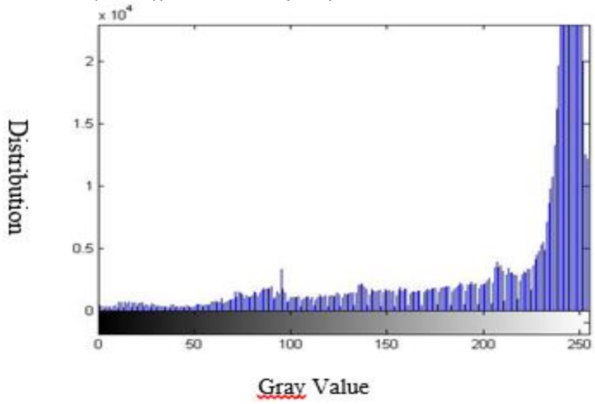
To prevent the brute force attack, a large key space should be employed [25]. The RC6-based HEVC SE technique uses RC6 block cipher with 128-bit secret key length. The key space size of the proposed method is $2^{128}$ which is very large and can ensure the robustness against the brute force attack.

### B. HISTOGRAMS ANALYSIS

The video frame histogram is a graphical representation of pixels distribution within the video frame at each colour intensity level. The histograms of ciphervideo frames should be different from the histograms of plainvideo frames [26]. Fig. 4 shows the histogram of the FourPepole plainvideo/ciphervideo frame number 50 by the RC6-based HEVC SE technique.




a) Histogram of FourPepole plainvideo Frame #50.




b) Histogram of FourPepole ciphervideo Frame # 50 using the proposed RC6-based HEVC SE technique.

Fig. 4. Histogram Analysis of FourPepole Plainvideo/Ciphervideo Frame # 50 Using the Proposed RC6-based HEVC SE Technique.

### C. CORRELATION COEFFICIENT ANALYSIS

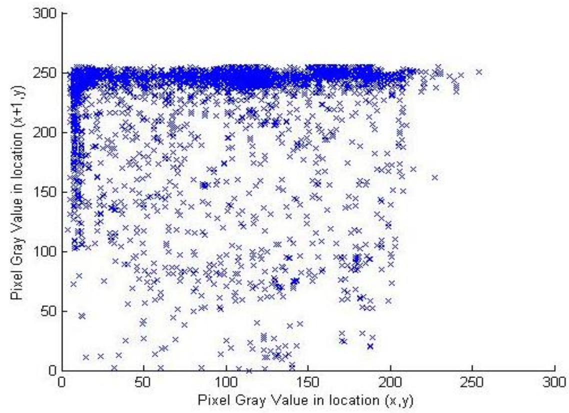
The Correlation coefficient metric can be defined as the measurement of the linear relationship between two variables. The correlation coefficient is widely utilized in the statistical analysis of the image processing to estimate the linear dependence among two adjacent pixels in the same image or two corresponding pixels in different images at the same position [27]. The correlation coefficient r can be estimated by the following equation [27]:

$$r_{mn} = \frac{\sum_{j}(m_j - m_k)(n_j - n_k)}{\sqrt{\sum_{j}(m_j - m_k)^2}\sqrt{\sum_{j}(n_j - n_k)^2}} \quad (1)$$

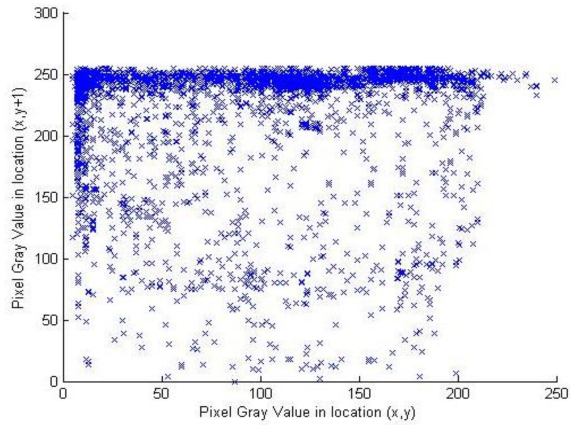
where, $m_j$ is the first pixel intensity value in position j and $m_k$ is the corresponding mean pixels intensity value in position j. $n_j$ is the second pixel intensity value in position j and $n_k$ is the corresponding mean pixels intensity value in position j. The m and n may represent the adjacent pixels in the same video frame or two corresponding pixels in different video frames at the same position j. For testing the correlation coefficient of the RC6-based HEVC SE technique, the following steps are employed:

- Selection of random 1000 pixels from the video frame #50 from the FourPeople plainvideo sequence.
- Selection of the corresponding 1000 pixels from the video frame #50 from the FourPeople ciphervideo sequence at the same positions.
- Calculating the correlation coefficient for the corresponding 1000 pixels using the formula in Eq. (1).

Fig. 5 shows the correlation distribution between the 1000 horizontally pixels in video frame #50 from the FourPeople plainvideo sequence and their corresponding pixels in the ciphervideo frame.

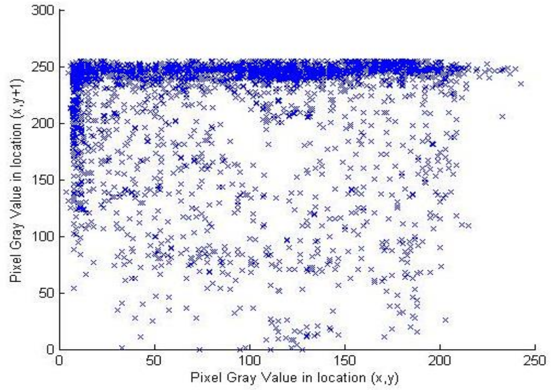



a) Horizontal Correlation of the FourPeople ciphervideo Frame # 50 using the proposed RC6-based HEVC SE technique = 0.0312.




b) Vertical correlation of the FourPeople ciphervideo Frame # 50 using the proposed RC6-based HEVC SE technique = 0.0750.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2017.2777470, IEEE Transactions on Multimedia




c) Diagonal Correlation of the FourPeople ciphervideo Frame # 50 Using the Proposed RC6-Based HEVC SE Technique = 0.0428.

Fig. 5. Correlation Distribution Between Pixels for the FourPeople plainvideo/ciphervideo Frame #50 Using the Proposed RC6-Based HEVC Technique.

a) The FourPeople plainvideo Frame # 50

b) The FourPeople ciphervideo Frame # 50 using the proposed RC6-based HEVC SE Technique with key "184467440737095"

c) The FourPeople ciphervideo Frame # 50 using the proposed RC6-based HEVC SE Technique with key "084467440737095"

Fig. 6. The Key Sensitivity Analysis of the FourPeople ciphervideo Frame # 50 Using the Proposed RC6-based HEVC SE Technique.

### D. Encryption Quality Analysis

With video encryption, there are a lot of changes in the pixel values in the ciphervideo frames compared with its corresponding pixels in the plainvideo frames. The video encryption quantity (EQ) calculates the average difference between the occurrence of each pixel gray level in the ciphervideo frames and the plainvideo frames [28]. The video encryption quantity (EQ) can be estimated by the following equation [28]:

$$EQ = \frac{\sum_{V=0}^{255} \left| G_V(R') - G_V(R) \right|}{256} \qquad (2)$$

where R' is denoted as the ciphervideo frame, R is denoted as the plainvideo frame and $G_V$ is denoted as the occurrence of each gray level V for the ciphervideo/plainvideo frame. Table 9 shows the encryption quality for the first 50 frames of the FourPepole ciphervideo sequence at different QP values and illustrates that the encryption remains in the higher range for these video frames.

TABLE 9: THE ENCRYPTION QUALITY FOR THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES FOR THE FOURPEOPLE VIDEO AT DIFFERENT QP VALUES.

| Technique / QP | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| **22** | 12819 | 6868 | 5528 | 7433 | 6868 | 6868 |
| **27** | 10338 | 4533 | 10052 | 7577 | 4533 | 4533 |
| **32** | 13738 | 15671 | 12720 | 9264 | 15671 | 15671 |
| **37** | 8344 | 10775 | 8606 | 11214 | 10775 | 10775 |

### E. Key Sensitivity Analysis

The HEVC SE technique should provide a high key sensitivity that means the ciphervideo cannot be decrypted correctly for a small change in the secret key that is used in the encryption process. The key sensitivity of the RC6-based HEVC SE technique grants the robustness against brute-force attacks. For testing the key sensitivity of the RC6-based HEVC SE technique, the following steps are employed:

- A video frame #50 from the FourPeople plainvideo sequence in Fig. 6(b) is ciphered by the proposed RC6-based HEVC SE technique with the secret key “184467440737095”.
- A video frame #50 from the FourPeople plainvideo sequence in Fig. 6© is ciphered by the proposed RC6-based HEVC SE technique with the secret key “084467440737095” (the most significant bit is changed in the secret key).

To ensure the difference between the ciphervideo frames, the correlation between the corresponding pixels at the same position in the ciphervideo frames is calculated is shown in Table 10. Fig. 7 shows that there is no correlation between the two ciphervideo frames although these have been encrypted by using small different secret keys values. So the RC6-based HEVC SE technique has high sensitivity towards slightly change in the secret key.

TABLE 10: THE CORRELATION COEFFICIENTS FOR THE FOURPEOPLE CIPHERVIDEO FRAME # 50 BY TWO DIFFERENT KEYS USING THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES.

| Correlation | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| Horizontal | 0.0312 | 0.1111 | 0.1420 | -0.2573 | 0.1111 | 0.1111 |
| Vertical | 0.0750 | 0.0543 | 0.1640 | -0.2530 | 0.0543 | 0.0543 |
| Diagonal | 0.0428 | 0.0784 | 0.1082 | -0.2140 | 0.0784 | 0.0784 |

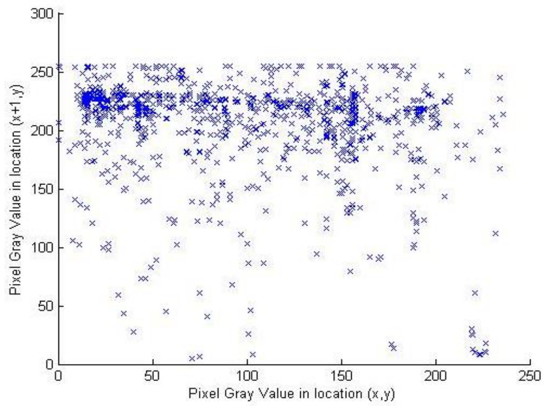



Fig. 7. The Horizontal Correlation for the FourPeople Ciphervideo Frame # 50 By Two Different Keys Using the Proposed Rc6-Based HEVC SE Technique.

### F. EDGES DETECTION PROTECTION

A good HEVC SE must protect the ciphervideo frame edges information from the attacks. The visual distortion of the RC6-based HEVC SE technique for a ciphervideo frame can be estimated by the distortion presented at the ciphervideo frame edges. The edge distortion can be estimated by the edge differential ratio (EDR) that can be defined by Eq. 3 [29]:

$$EDR = \frac{\sum_{m,n=1}^{N} \left| P(m,n) - \overline{P}(m,n) \right|}{\sum_{m,n=1}^{N} \left| P(m,n) + \overline{P}(m,n) \right|} \qquad (3)$$

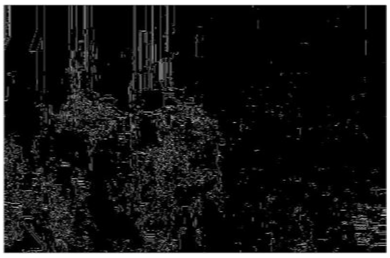
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2017.2777470, IEEE Transactions on Multimedia

where $P(m,n)$, $\overline{P}(m,n)$ are the values of the pixel values in the edge for the plainvideo and ciphervideo frames. Table 11 shows that the EDR between the plainvideo and ciphervideo frame #50 from the FourPeople video sequence using the proposed RC6-based HEVC SE technique is 0.9455 and close to 1 that ensures that the plainvideo and ciphervideo frames are different. Fig. 8 shows the Laplacian of Gaussian edge detection for the plainvideo/ciphervideo frames.

TABLE 11: THE EDR FOR THE ENCRYPTED FOURPEOPLE VIDEO FRAME # 50 USING THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES.

| Technique | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| EDR | 0.9455 | 0.9462 | 0.9333 | 0.9251 | 0.9462 | 0.9462 |

a) Edge Detection of the FOURPEOPLE PLAINVIDEO FRAME # 50



b) Edge Detection of the FOURPEOPLE CIPHERVIDEO FRAME # 50

Fig. 8: Laplacian of Gaussian Edge Detection of the FourPeople Plainvideo/ciphervideo Frames # 50 Using the Proposed RC6-based HEVC SE Technique.

## G. INFORMATION ENTROPY ANALYSIS

The information entropy metric is the probability of occurrence for each symbol in the video frame [30]. The entropy is defined by Eq. 4 [30]:

$$E(n) = \sum_{i=0}^{2^N-1} p(n_i)\log_2 \frac{1}{p(n_i)} \quad bits, \qquad (4)$$

where E(n) denotes the entropy of $n$ and $P(n_i)$ is the probability of occurrence of symbol $n_i$ in $n$. The entropy value should be 8 for the truly random frame.

TABLE 12: THE INFORMATION ENTROPY FOR THE ENCRYPTED FOURPEOPLE VIDEO FRAME # 50 USING THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES.

| Technique / QP | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| 22 | 7.2888 | 7.6125 | 7.7295 | 7.3097 | 7.6125 | 7.6125 |
| 27 | 7.4615 | 7.6492 | 7.7560 | 7.5783 | 7.6492 | 7.6492 |
| 32 | 6.3048 | 5.4838 | 7.1531 | 7.2904 | 5.4838 | 5.4838 |
| 37 | 7.5718 | 7.4634 | 7.4878 | 7.3417 | 7.4634 | 7.4634 |

Table 12 shows the entropy of FourPeople ciphervideo frame #50 at different QP by the RC6-based HEVC SE technique. The estimated entropy is near to the theoretical value 8. This means the RC6-based HEVC SE technique is secure and robust against the entropy attack.

## H. Cipher Cycle Analysis

The ciphervideo should be different from its respective plainvideo. To ensure this requirement, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI) measures can be utilized [31-32]. The NPCR estimates the difference in pixels of the colour components between two videos frames. The UACI estimates the average intensity differences in a colour component between two videos frames. The NPCR and UACI are defined as [31-32]:

$$NPCR = \frac{\sum_{m,n} E(m,n)}{X \times Y} \times 100\%, \qquad (5)$$

$$UACI = \frac{1}{X \times Y}\left[\sum_{m,n} \frac{F_1(m,n) - F_2(m,n)}{255}\right] \times 100\%, \qquad (6)$$

where $F_1$ and $F_2$ are the two different video frames. The X and Y are the width and height of $F_1$ or $F_2$. The E(i, j) = 1 if $F_1$ (m, n) = $F_2$ (m, n) otherwise, E(m, n) = 0. The results from NPCR and UACI in Tables 13 and 14 indicate that the RC6-based HEVC SE technique gives highly difference in pixels of the colour components between the ciphervideo and plainvideo frames.

TABLE 13: THE NPCR FOR THE FOURPEOPLE CIPHERVIDEO FRAME # 50 USING THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES.

| Technique / QP | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| 22 | 99,77 | 99,41 | 99,47 | 99,57 | 99,41 | 99,41 |
| 27 | 98,59 | 98,92 | 99,68 | 99,55 | 98,92 | 98,92 |
| 32 | 99,79 | 99,80 | 99,81 | 99,38 | 99,80 | 99,80 |
| 37 | 99,71 | 99,73 | 99,71 | 99,31 | 99,73 | 99,73 |

TABLE 14: THE UACI FOR THE FOURPEOPLE CIPHERVIDEO FRAME # 50 USING THE PROPOSED AND THE PREVIOUS RELATED SE TECHNIQUES.

| Technique / QP | RC6 | AES_CFB | AES_CBC | AES_ECB | AES_OFB | AES_CTR |
|---|---|---|---|---|---|---|
| 22 | 48,19 | 32,17 | 26,04 | 33,03 | 32,17 | 32,17 |
| 27 | 30,96 | 27,24 | 44,38 | 32,87 | 27,24 | 27,24 |
| 32 | 46,88 | 45,47 | 45,09 | 32,83 | 45,47 | 45,47 |
| 37 | 38,23 | 35,88 | 38,45 | 35,93 | 35,88 | 35,88 |

# V. CONCLUSION

This paper presented an overview of the binarization process in the entropy stage of the HEVC video coding structure and introduced the differences between the various binarization methods. It also presented an efficient RC6-based HEVC SE technique to encrypt the DCT coefficients sign bits, the DCT remaining absolute value suffixes that are binarized by EG0, the MVD sign bits and MVD absolute value suffixes that are binarized by EG1. The RC6-based HEVC SE technique encrypts these syntax elements because any modification of the suffix and the sign bin has no effect on the HEVC video format compliance and bit rate. The RC6-based HEVC SE technique utilizes the RC6 block cipher which is fast and simple encryption structure to save the conversion time of non-dyadic encryption space to dyadic encryption space process in Z. Shahid [9] algorithm due to using the AES-CFB and hence ensures the real-time constraint.

A comparison between the RC6-based HEVC SE technique and the previous related work that uses the AES in different operation modes like CFB, CBC, ECB, OFB and CRT was presented in this paper. The experimental results showed that the proposed method saved the average encoding time for one frame by 0.7 sec and 4.4 sec compared with AES-CFB and AES-CBC, respectively for the low-resolution Forest

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2017.2777470, IEEE Transactions on Multimedia

video (320 X 240). Also, the RC6-based HEVC SE technique saves the average encoding time for one frame by 19 sec and 211 sec compared with AES-CFB and AES-CBC for the high-resolution Bosphorus video (3840 X 2160). This saving in the encoding time is due to the simple and low complexity of using RC6 cipher block instead of using the AES in the previous related work for HEVC SE. Also, the paper presented the security analysis of the RC6-based HEVC SE technique including the key space analysis, encryption quality analysis, statistical analysis and sensitivity analysis. The security analysis experimental results demonstrated and proved that the RC6-based HEVC SE technique is highly secure and robust against different types of attacks.

## REFERENCES


[1] B. Bross, "High Efficiency Video Coding (HEVC) text specification draft 8," JCTVC-J1003, Joint Collaborative Team on Video Coding of ITU-T SG16 WP3 and ISO/IEC JTC1/SC29/WG11, 10th Meeting: Stockholm, SE, Jul. 2012.

[2] M. Wang, K.Ngan, L. Xu, "Efficient H.264/AVC Video Coding with Adaptive Transforms," IEEE Transactions On Multimedia, Vol. 16, No. 4, June 2014, pp. 933–946.

[3] D. Souza, A. Ilic, N. Roma, L. Sousa, "GHEVC: An Efficient HEVC Decoder for Graphics Processing Units," IEEE Transactions On Multimedia, Vol. 19, No. 3, March 2017, pp. 459 - 474.

[4] Y. Gao, P. Liu, Y. Wu, K. Jia, "Quadtree Degeneration for HEVC," IEEE Transactions On Multimedia, Vol. 18, No. 12, 2016, pp. 2321 - 2330.

[5] W. Shen, Y. Fan, Y. Bai, L. Huang, Q. Shang, C. Liu, X. Zeng, "A Combined Deblocking Filter and SAO Hardware Architecture for HEVC," IEEE Transactions On Multimedia, Vol. 18, No. 6, 2016, pp. 1022 - 1033.

[6] F. Bossen, B. Bross, K. Suhring, D. Flynn, "HEVC Complexity and Implementation Analysis," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 22, No. 12, December 2012, pp. 1685-1696.

[7] H. Hofbauer, A. Unterweger, and A. Uhl,"Transparent Encryption for HEVC Using Bit-Stream-Based Selective Coefficient Sign Encryption,"Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), May 2014, pp.1986–1990.

[8] Y. Tew, K. Minemura and K. Wong, " HEVC Selective Encryption using Transform Skip Signal and Sign Bin," Proceedings of APSIPA Annual Summit and Conference 2015, December 2015, pp.963–970.

[9] Z. Shahid and W. Puech," Visual Protection of HEVC Video by Selective Encryption of CABAC Binstrings," IEEE Transactions on Multimedia, Vol. 16, No. 1, January 2014, pp.24-36.

[10] NIST, "Advanced encryption standard (AES)," FIPS Publication 197, Nov. 2001.

[11] G. Wallendael, A. Boho, J. Cock, A. Munteanu and R. Walle "Encryption for High Efficiency Video Coding with Video Adaptation Capabilities", Proceedings of IEEE Transactions on Consumer Electronics, Vol. 59, No. 3, August 2013, pp. 634-642 .

[12] V. Sze and D. Marpe, "Entropy Coding in HEVC," chapter 8 in High Efficiency Video Coding (HEVC) Algorithms and Architectures Handbook, Springer, International Publishing Switzerland, 2014.

[13] https://en.wikipedia.org/wiki/Exponential-Golomb_coding, Access Date: 1/9/2016.

[14] S. Contini, R. Rivest, M. Robshaw, and Y. Yin, "The Security of The RC6TM Block Cipher," RSA Laboratories, M.I.T laboratory for Computer Science, Version 1.0 - August 20, 1998.

[15] R. Rivest, M. Robshaw, R. Sidney, and Y. Yin, "The RC6 Block Cipher: A Simple Fast Secure AES Proposal," M.I.T Laboratory for Computer Science, RSA Laboratories, USA, August 21, 1998. Available at: http://csrc.nist.gov/CryptoToolkit/aes/round1/conf1/rc6-slides.pdf.

[16] J. Daeman and V. Rijmen, "AES proposal: Rijndael," 1999. Available at: http://www.esat.kuleuven.ac.be/~rijmen/rijndael/rijndaeldocV2.zip, Access Date: 1/9/2016.

[17] B. Gladman, "A Specification for Rijndael, The AES Algorithm," 2003. Available at: ftp.gladman.plus.com/cryptography_technology/ rijndael/, Access Date: 1/9/2016.

[18] http://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm, Access Date: 1/9/2016.

[19] https://www.tutorialspoint.com/cryptography/block_cipher_modes_of_operation.htm, Access Date: 1/9/2016.

[20] G. Bjøntegaard, "Calculation of average PSNR differences between RD-curves," document VCEG-M33 of ITU-T Video Coding Experts Group (VCEG), Apr. 2001.

[21] Fraunhofer Heinrich Hertz Institute. (2015), High Efficiency Video Coding: HEVC software repository [Online]. Available: https://hevc.hhi.fraunhofer.de.

[22] https://media.xiph.org/, Access Date: 1/6/2016.

[23] http://ultravideo.cs.tut.fi/#testsequences, Access Date: 1/6/2016.

[24] MSU Graphics and Media Lab, Video Group, MSU codecs, www.compression.ru/ video/, Access Date: 1/6/2016.

[25] H. Ahmed, H. Kalash and O. Farag Allah "An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for image encryption and decryption", Proceedings of Informatica, Vol. 31, No 1, Mar 2007, pp. 121-129.

[26] J. Ahmad and F. Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", Proceedings of International Journal of Video & Image Processing and Network Security, Vol. 12, No. 04, 2012, pp. 18-31.

[27] A. Kaur, L. Kaur and S. Gupta "Image Recognition using Coefficient of Correlation and Structural SIMilarity Index in Uncontrolled Environment", Proceedings of International Journal of Computer Applications, Vol. 59, No. 5, 2012, pp. 32-39.

[28] A. Jolfaei and A. Mirghadri "A New Approach to Measure Quality of Image Encryption", Proceedings of International Journal of Computer and Network Security, Vol. 2, No. 8, 2010, pp. 38-43.

[29] http://www.mathworks.com/help/images/ref/edge.html, Access Date: 1/6/2016.

[30] https://www.codementor.io/tips/9423772841/how-to-calculate-the-shannon-entropy-of-a-part-of-image-data, Access Date: 1/6/2016.

[31] Y. Mao, G. Chen, and S. Lian, "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps," Int. J. Bifurcation and Chaos, 14(10), pp. 3613–3624, 2004.

[32] Y. Mao, G. Chen, and C. Chui, "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps," Chaos, Solitons & Fractals, 21(3), pp.749–761, 2004.


**Eng. Ahmed I. Sallam** was born in AL gharbia, Egypt on April 10, 1982. He received a B.S. in Computer Science & Engineering (2005) from Al Azhar University, Faculty of Engineering. He received M.sc Computer Science & Engineering (2012) from Menoufia University, Faculty of Electronic Engineering. He became a Software Development Team Leader in Qarun Petroleum Company. His research interests cover Database Security, Cryptography, Internet Security and Multimedia Security.

**Prof. El-Sayed M. EL-Rabaie** was born in Sires Elian, Egypt, in 1953. He received the B.Sc. degree (with honors) in radio communications from Tanta University, Tanta, Egypt, in 1976, the M.Sc. degree in communication systems from Menoufia University, Menouf, Egypt, in 1981, and the Ph.D. degree in microwave Device engineering from Queen’s University of Belfast, Belfast, U.K., in 1986. In his doctoral research, he constructed a Computer-Aided Design (CAD) package used in nonlinear circuit simulations based on the harmonic balance techniques. Up to February 1989, he was a Postdoctoral Fellow with the Department of Electronic Engineering, Queen’s University of Belfast. He was invited as a Re-search Fellow in the College of Engineering and Technology, Northern Arizona University, Flagstaff, in 1992 and as a Visiting Professor at Ecole Polytechnique de Montreal, Montreal, QC, Canada, in 1994. He has authored and Co-authored of More Than 300 Papers and nineteen text Books. He acts as a reviewer and member of the editorial board for several scientific journals. He Has Shared in Translating the First Part of the Arabic Encyclopedia. Professor EL-Rabaie was the Head of the Electronic and Communication Engineering Dept., Faculty of Electronic Engineering, Menoufia University, then the Vice Dean of Postgraduate Studies and Research in the same Faculty.

**Osama S. Faragallah** received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in Computer Science and Engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. He is currently Associate Professor with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he was a Demonstrator from 1997 to 2002 and has been Assistant Lecturer from 2002 to 2007 and since 2007 he has been a Teaching Staff Member with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. He is a coauthor of about 150 papers in international journals and conference proceedings, and two textbooks. His current research interests include network security, cryptography, internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, and chaos theory. Email: osam_sal@yahoo.com, o.salah@tu.edu.sa.